



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1150
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/618,861	07/14/2003	Eric Balard	TI-34921	6971

23494 7590 04/10/2006

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER

HO, THOMAS M

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 04/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/618,861	BALARD ET AL.	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 July 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☒ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>12/1/03</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-12 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 4-7, 10-12 are rejected under 35 U.S.C. 102(e) as being anticipated by Gray, US patent, 6268788.

In reference to claim 1:

Gray (Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10) &

Figure 4 discloses a method of securing access to resources in a computing device, comprising the steps of:

- Storing an encrypted access code in a known memory location with the computing device; (Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10)

- Receiving a password to access the resources; (Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10)
- Encrypting the password to produce the encrypted access code; (Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10)
- Allowing access to the resources if the encrypted access code matches the encrypted password. (Column 6, lines 16-20) & (Column 6, line 65- Column 7, line 5)

In reference to claim 4:

Gray (Column 5, lines 62- Column 6, lines 20) & (Column 9, lines 53-65) discloses the method of claim 1 wherein the encrypted access code is stored in a memory that cannot be externally modified, where the information stored on the computer system cannot be captured or tampered with and is stored in a secure room.

In reference to claim 5:

Gray (Column 6, lines 55-Column 7, line 10) discloses the method of claim 1 wherein the step of allowing access comprises the step of allowing access to testing resources if the encrypted access code matches the encrypted password.

In reference to claim 6:

Gray (Column 6, lines 55-Column 7, line 10) discloses the method of claim 1 wherein the step of allowing access comprises the step of allowing access to change system parameters if the encrypted access code matches the encrypted password.

In reference to claim 7:

Gray (Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10) & Figures 2, 4 discloses a computing device comprising:

- A processing system (Figure 2, Items 40 and Items 60)
- A memory for storing an encrypted access code; (Figure 2, Items 42 and Items 62)
- Input circuitry for receiving a password to access the resources; (Figure 2, Items 16 and Items 34)
- Wherein the processing circuitry:
 - Encrypts the password to produce a encrypted password; (Column 6, lines 1-8) & (Column 6, lines 55-Column 7, line 10)
 - Compares the encrypted password to the encrypted access code; (Column 6, lines 1-8) & (Column 6, lines 55-Column 7, line 10)
 - Allows access to the resources if the encrypted access code matches the encrypted (Column 6, lines 55-Column 7, line 10)

In reference to claim 10:

Gray (Column 5, lines 62- Column 6, lines 20) & (Column 9, lines 53-65) discloses the computing device of claim 7 wherein the encrypted access code is stored in a memory that cannot be externally modified, where the information stored on the computer system cannot be captured or tampered with and is stored in a secure room.

In reference to claim 11:

Gray (Column 6, lines 55-Column 7, line 10) discloses the computing device of claim 7 wherein the processing system allows access to testing resources if the encrypted access code matches the encrypted password.

In reference to claim 12:

Gray (Column 6, lines 55-Column 7, line 10) discloses the computing device of claim 7 wherein the processing system allows access to system parameters if the encrypted access code matches the encrypted password.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 2,3,8,9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray and Lohstroh et al, US patent 5768373.

In reference to claims 2, 3, 8, 9:

Art Unit: 2134

Gray fails to explicitly disclose the method of claim 1 wherein the step of storing an encrypted access code comprises the step of storing a hashed access code.

Lohstroh, paragraph 15 teaches

*(15) The encryption/decryption algorithm performed by units 252 and 258 is symmetric. Thus, since K.sub.acc is supplied to encryption unit 252, K.sub.acc must also be supplied to decryption unit 258. Yet, as with other keys, if K.sub.acc is stored in plaintext form in non-volatile storage means, and sometime later an unauthorized person discovers the location of K.sub.acc, the security of data will be compromised as other encrypted keys will then become accessible. Therefore, access key K.sub.acc is supplied on line 232 to encrypting unit 234 which operates according to well-known symmetric encryption/decryption algorithms such as "Blowfish", which can generally be found in Bruce Schneier, Applied Cryptography (2d.Ed. 1995). The resulting encrypted signal *K.sub.acc1 * produced on line 236 is stored in storage region 238. The key signal that is applied to encrypting unit 234 on line 264 is K.sub.pwh and is produced by hashing unit 262 from a user-supplied password on line 261. "Hashing" is generally the using of an algorithm to take a variable size input and produce a unique fixed-length identifier representative of the original input (here, the user password). One hash algorithm, MD5, or message digest 5, is generally known in the art, and is suitable for hashing a user password. Other algorithms are also generally known and are also suitable for*

hashing a user password in accordance with the invention. Often hash functions are thought to take a large block of data and reduce it to a smaller block. However, because the user password can vary from a few characters to up to 99 bytes in one embodiment, hash function 262 may produce a larger or smaller block of data than a given input (the user password), but it will return a password hash (K.sub.pwh) of consistently fixed length. In one embodiment using the MD5 hash function, such fixed length is set to 16 bytes.

Thus Lohstroh teaches an embodiment where an access key or “access code” is encrypted by first hashing it.

“The key signal that is applied to encrypting unit 234 on line 264 is K.sub.pwh and is produced by hashing unit 262 from a user-supplied password on line 261.”

Lohstroh also teaches that the password can vary from a few characters up to 99 bytes, but after the hash, it will return a password hash of consistently fixed length.

It would have been obvious to one of ordinary skill in the art at the time of invention to use a hash as a step in a cryptographic process to encrypt the hash in order to reduce a variable length password into a fixed length, providing for greater password security by masking the length of and number of characters within the password.

Conclusion

6. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 571-273-8300
Customer Service Representative	Telephone: 571-272-2100	Fax: 571-273-8300

TMH

March 6th, 2006

Thomas M Ho AU 2134

E. L. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER